Remark

Applicants respectfully request reconsideration of this application as amended. Claims 1 and 11 are amended. Claims 1 and 11, as amended, refer to generating a configuration baseline and a file system database. The elements were not previously claimed and further distinguish the invention over the references.

Conclusion

Applicants respectfully submit that the claims as amended are now in condition for allowance. Accordingly, Applicants respectfully request the rejections be withdrawn and the claims as amended be allowed.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 7/13/11

Gordon R. Lindeen III
Reg. No. 33,192

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1026
(303) 740-1980

Version with Markings to Show Changes Made

Insertions are underlined, deletions are bracketed.

1. (Amended) A security system for a computer apparatus, wherein said computer apparatus includes a processor and system memory, said security system comprising:

at least one security module which under direction from the processor accesses and analyzes selected portions of the computer apparatus to identify vulnerabilities;

at least one utility module which under the direction from the processor, performs various utility functions with regards to the computer apparatus in response to the identified vulnerabilities, the utility functions including generating a configuration baseline and a file system database for use in performing other utility functions; and

a security system memory which contains security information for performing the analysis of the computer apparatus.

11. (Amended) A method of providing a security assessment for a computer system which includes a system memory, comprising the steps of:

generating a configuration baseline;

providing a security subsystem in the computer system such that functionality of the security subsystem is directed through a processor for the computer system, wherein the security performs steps comprising:

identifying a configuration of system and generating a file system database;

accessing the system memory and performing at least one procedure to provide a security assessment for at least one aspect of the computer system;

as a result of any vulnerabilities discovered in the assessment, identifying corrective measures to be taken with regards to the computer system;

reporting the discovered vulnerability and the identified corrective measures; and upon receiving an appropriate command, initiating the corrective measures.